Everything you need to know about cyber risks, resilience and responsibilities

Allens Linklaters | 200

A GUIDE FOR BOARDS AND SENIOR MANAGEMENT

Businesses today are both blessed and cursed with extraordinary amounts of data.

On the one hand, this presents exciting opportunities to personalise offerings, automate processes and extract other benefits from this incredibly valuable asset class.

On the other hand, businesses are facing:

- unprecedented regulatory reform and regulator scrutiny;
- consumer and investor demands for greater transparency about the way their data is used and protected, and the way organisations respond to data breaches; and
- heightened financial, operational and reputational threats posed by sophisticated and determined threat actors.

Where, then, does responsibility for information security and data governance lie?

Put simply, it starts and ends with the board and senior management. This is being reinforced by a host of regulators that are applying growing pressure to organisations to uplift their practices or face financial penalties, regulatory action, eroded consumer trust and reputational damage.

This handbook is designed to help boards and senior management navigate their duties and liabilities relating to information security and data risk.

For a comprehensive list of questions directors should be asking to inform themselves about the cyber risks faced by their organisation, read our checklist *Questions boards should be asking about cyber risks, readiness and resilience.*

> *Boards need to have a thorough understanding of their risks, and how to mitigate against, and recover from cyber incidents – this is now fundamental to business risk management and potential survival*
>
> *– ASIC Commissioner John Price*[1]

Key takeaways

The global cost of cybercrime is predicted to reach $10.5 trillion annually by 2025[2]

1 Directors will be held to account for cybersecurity failures

Directors may be *personally liable*, and face disqualification and/or reputational damage, for cybersecurity failures that result in regulatory breaches (direct and ancillary). Directors' acts or omissions may also *contribute to the liability of organisations*, particularly in circumstances where regulators (including ASIC, APRA and the OAIC) have repeatedly emphasised the criticality of board-level oversight of cyber and data risk issues.

2 Boards should help define their company's cyber risk appetite

Boards should also ensure they are briefed on cyber risk assessments undertaken by the company. This will help ensure that any actions taken are in line with the interests of the company.

3 Regulators expect that organisations will:

- have adequate cybersecurity and resilience risk management *systems, controls, documentation and resources* (financial, technological and human), to ensure they are not exposing the company (or individuals and other customers to whom financial services are supplied) to an unacceptable level of risk;
- ensure there is adequate awareness of these measures within the company; and
- test these measures on a regular basis, to ensure they are effective and remain fit for purpose.

4 Directors need to consider readiness for, and response to, cyberattacks

Compliance with directors' duties will require directors to: (a) understand cyber risks and the operational, financial and reputational impact on the company if those risks eventuate; (b) consider what systems and processes should be put in place to ensure the company is prepared to address these cyber risks on an *ongoing basis*; and (c) determine how the organisation should respond in the heat of a crisis to protect the interests of the company.

5 Organisations are facing greater scrutiny of cybersecurity disclosures

We expect to see regulators increasingly take enforcement action for delayed, misleading and deficient notifications, and inadequate notification policies and procedures that sit behind them.

6 Directors should consider whether specific cybersecurity expertise is required on the board

Cybersecurity awareness needs to be uplifted across the board, given the increasing focus on the composition and cyber maturity of boards.

7 Cyber resilience and data governance should form part of an organisation's ESG agenda

Greater awareness of the social impact of cyberattacks and unethical data-handling practices is fuelling consumer and regulator demands for sound cyber and data governance and greater transparency.

8 Board members should ensure their company has a regularly tested ransomware response plan in place

The plan should include a process for briefing the board and clear authorities for critical ransomware decisions. Almost 33% of all companies experienced at least one cyber ransom incident in 2021. Ransomware attacks cost businesses more than $20 billion, up from $325 million in 2015 (a 57x increase).[3]

Table of contents

Contents

1. Directors will be held to account for cybersecurity failures

In light of evidence that boards frequently don't understand, or are not adequately informed about cyber risks, we're no longer prepared to simply take their words for it – we want compliance independently verified... If boards are unwilling or unable to make the required changes in a timely manner, we will consider using formal enforcement action.

– APRA executive board member Geoff Summerhayes[4]

Regulators can hold directors to account (both directly and indirectly) for failure to appropriately manage cyber and data risks in a number of ways.

Personal liability

Directors may be personally liable for:

- breaches of director's duties. Directors or officers of a corporation may be found to have breached their duty to act with due care and diligence (or another statutory duty) for failing to prevent a reasonably foreseeable risk of harm to the corporation as a result of a contravention of legal or regulatory requirements;[5]
- involvement in breaches of continuous disclosure and other reporting obligations (eg a failure to disclose a cyberattack that would reasonably be expected to have a material effect on the price of a listed entity's securities);[6]
- involvement in misleading or deceptive conduct[7] (eg where an organisation's public documentation, such as a privacy policy or ASX disclosures, include misleading statements as to how the organisation protects personal information, or is handling a potential or actual cyberattack or data breach). The accuracy of public statements is actively enforced by ASIC; and
- misleading regulators, including through attestations in relation to compliance with risk management programs.

Personal accountability

Regulators, including APRA, ASIC, and the OAIC, expect organisations to hold senior management and the board accountable for effective risk management.

Accessorial liability

Though harder to prove, directors may also be subject to claims of accessorial liability for breaches by organisations (eg for being knowingly concerned in serious or repeated interferences with privacy under the *Privacy Act 1988 (Cth)).*[8]

Attributing and aggravating corporate liability

Board-level knowledge of compliance and risk management issues that are not swiftly and decisively addressed, or the failure of a board to be informed of serious longstanding issues, increases the seriousness of corporate misconduct and, in the case of some offences, can be the basis of attributing liability to a corporation. In turn, this increases the likelihood of court-based enforcement and the severity of the penalties imposed.

Directors can expect their state of mind and oversight of management to be closely examined in any enforcement proceedings. This is particularly the case for cyber risk issues, given that both APRA and ASIC have made it clear that there should be board oversight.

Class action risk

With reforms to the Privacy Act on the horizon, privacy and data breach class action risk remains an area to watch.

Penalties for civil breaches can be $1.1 million or three times the benefit derived or detriment avoided. In particularly egregious cases, various criminal offences with penalties involving imprisonment could be pursued.[9]

There are significant time pressures for decision making when responding to a cyber security incident. As a board, you should ensure you are available and prepared to make critical decisions that might exceed the delegated authority of executives and update your organisation risk appetite statement as required by a dynamic situation.

– ACSC[10]

2. The current challenge

When it comes to data and cyber resilience, organisations and their boards face a number of challenges in managing cyber risk, avoiding disruption to services, and complying with regulatory obligations.

Volume, pace and complexity of regulatory reform

It is becoming increasingly difficult to navigate the growing patchwork of data regulatory regimes. Not only do organisations need to contend with the volume and pace of new data regulatory developments, they also have to apply existing regimes in Australia, many of which were not originally intended to address cybersecurity. This creates significant compliance challenges.

Increased regulator scrutiny

Yet compliance is essential, as regulators (which in Australia include the OAIC, ACCC, ASIC, APRA and FIRB) are increasingly scrutinising data handling and cybersecurity practices, and using their expanding enforcement arsenal to hold organisations to account in unprecedented ways.

Heightened threat landscape

Cybersecurity incidents are costing the Australian economy an estimated $29 billion annually, as the frequency, scale, sophistication and severity of these incidents continues to escalate.

The commercial imperative

Individuals now expect greater transparency about, and control over, their data. Effective data governance is an essential part of building and sustaining stakeholder and consumer trust.

Regulators are alive to these challenges but they also expect organisations – and their boards – to manage them. These days, having an effective, comprehensive whole-of-business cyber and data strategy and framework in place is the only way to maximise the value of data and cyber resilience, comply with changing regimes, and avoid personal and organisational liability.

> *"We identified at least 51 Commonwealth, state and territory laws that create, or could create, some form of cyber security obligation for businesses."*
>
> *– Strengthening Australia's cyber security regulations and incentives discussion paper*[11]

3. What do regulators expect...

FROM BOARDS

Each of ASIC, APRA and the OAIC has confirmed that boards are ultimately responsible for data and information security governance. With directors now personally liable for regulatory breaches (both direct and ancillary), they should ensure:

- ☐ Board-level oversight (including regular reporting) and that they have a deep understanding of the cyber risks faced by their organisations
- ☐ Cyber risk assessments are undertaken, the cyber risk appetite is defined, and appropriate cyber governance and risk management systems are implemented to identify and manage cyber risks (including regulatory risks)
- ☐ Their organisation can withstand and recover from a major cyberattack
- ☐ Timely and adequate disclosures of cyber incidents are made in line with regulatory obligations
- ☐ Data assets are leveraged in a compliant and ethical manner

> *It is ultimately the board's responsibility to ensure that management is fully across the cyber threat they face and, where necessary, takes appropriate action to ensure its entity remains cyber resilient.*
>
> *– APRA*[12]

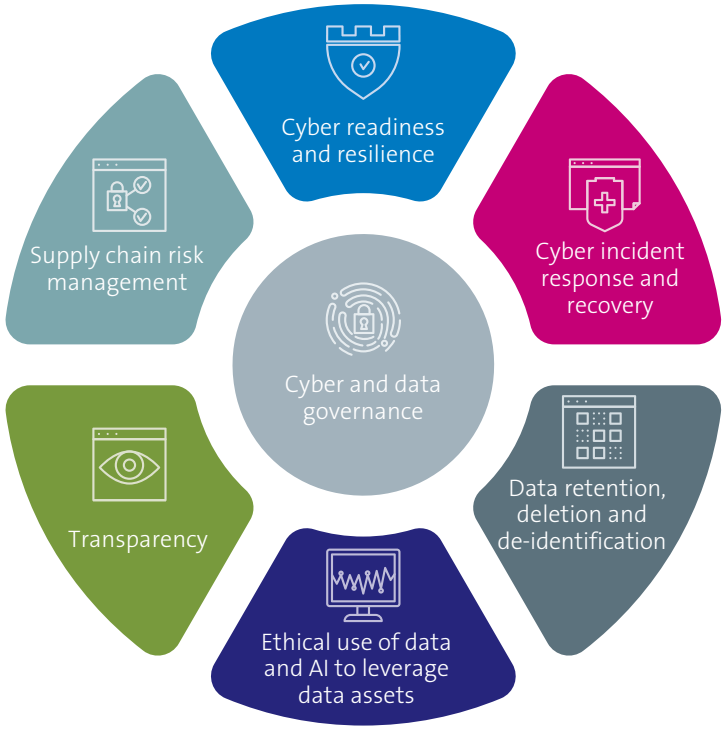
FROM ORGANISATIONS

Regulators expect that your organisation:

- ☐ has an overarching, cohesive, documented, information security program or roadmap to assess cyber risk and improve cybersecurity posture and preparedness for a cyberattack
- ☐ implements appropriate technical and operational controls, and creates the documentation to support them
- ☐ manages third-party risk throughout the lifecycle of third-party arrangements (including by doing *due diligence* on providers, appropriately *classifying the risk* that they pose, setting *baseline technical and operational requirements,* applying *compensating controls* where necessary, and also *monitoring and assessing compliance* with those requirements and controls on an ongoing basis)
- ☐ is able to withstand and recover from disruption, ensure the continuity of key services, and do all of this with as little impact as possible on consumers
- ☐ has systems in place to quickly identify and internally escalate issues, and to notify relevant regulators and other key stakeholders where required
- ☐ ensures that its people are aware of its controls, policies and processes, including via regular roles-based training
- ☐ tests its controls and documentation
- ☐ monitors and reports on compliance with its program and cybersecurity framework
- ☐ hires and retains enough staff to appropriately manage technology and risk issues
- ☐ ensures the board and management have oversight and accountability over the whole program or roadmap

> *The ASX's Cyber Health Check survey of Australia's top 100 listed companies found that only 34% of boards had clearly defined risk appetite for cyber and only 11% had a clear understanding of where the company's key information or data assets were being shared with another provider.*[13]

KEY REGULATORY TRENDS



4. Spotlight: Critical infrastructure

The bill proposes that the risk management program is reported to a critical infrastructure assets board, council or governing body. This ensures that the material risks in the functioning of the asset are reported and raised with the most senior levels of critical infrastructure assets. Organized cybercrime entities are joining forces, and they likelihood of detection and prosecution is estimated to be as low as 0.05% in the United States.

– Hon Karen Andrews MP, Second Reading speech (Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022)[14]

APRA expects boards to have the same level of confidence in reviewing and challenging information security issues as they do when governing other business issues.

– APRA[15]

As threat actors increasingly turn their attention to critical infrastructure (for their disruptive and espionage potential), governments globally are intensifying their regulation of these assets as a key part of their national security strategy.

In Australia, recent amendments to the *Security of Critical Infrastructure Act 2018* (***SOCI Act***) introduce new obligations for responsible entities that should be front of mind for their boards. This includes:

- implementing and maintaining a Risk Management Program to manage and mitigate prescribed risks associated with their critical infrastructure asset;
- observing enhanced cybersecurity obligations for assets declared by the Minister to be 'systems of national significance', which may involve adopting and maintaining incident response plans, undertaking cybersecurity exercises, reporting on vulnerability assessments, and providing the government with access to system information;
- registering their asset on the Register for Critical Infrastructure Assets. At the moment this obligation applies only to some sectors, including electricity, gas, ports, water, broadcasting, data storage, food and grocery, freight, public transport and energy;
- complying with any government assistance measures, including a direction from the Secretary of the Department of Home Affairs to provide information, act in a specific way to mitigate national security risks, or permit the Australian Signals Directorate (ASD) to step in and take direct action where necessary; and
- notifying the ASD of a cyber security incident within 12 or 72 hours, depending on the level of impact it is having on the business.

SECTORS REGULATED BY THE SOCI ACT

- Communications
- Data storage or processing
- Financial services and markets
- Water and sewerage
- Energy
- Health care and medical
- Higher education and research
- Food and groceries
- Transport
- Space technology
- Defence

5. Global developments

Overseas developments

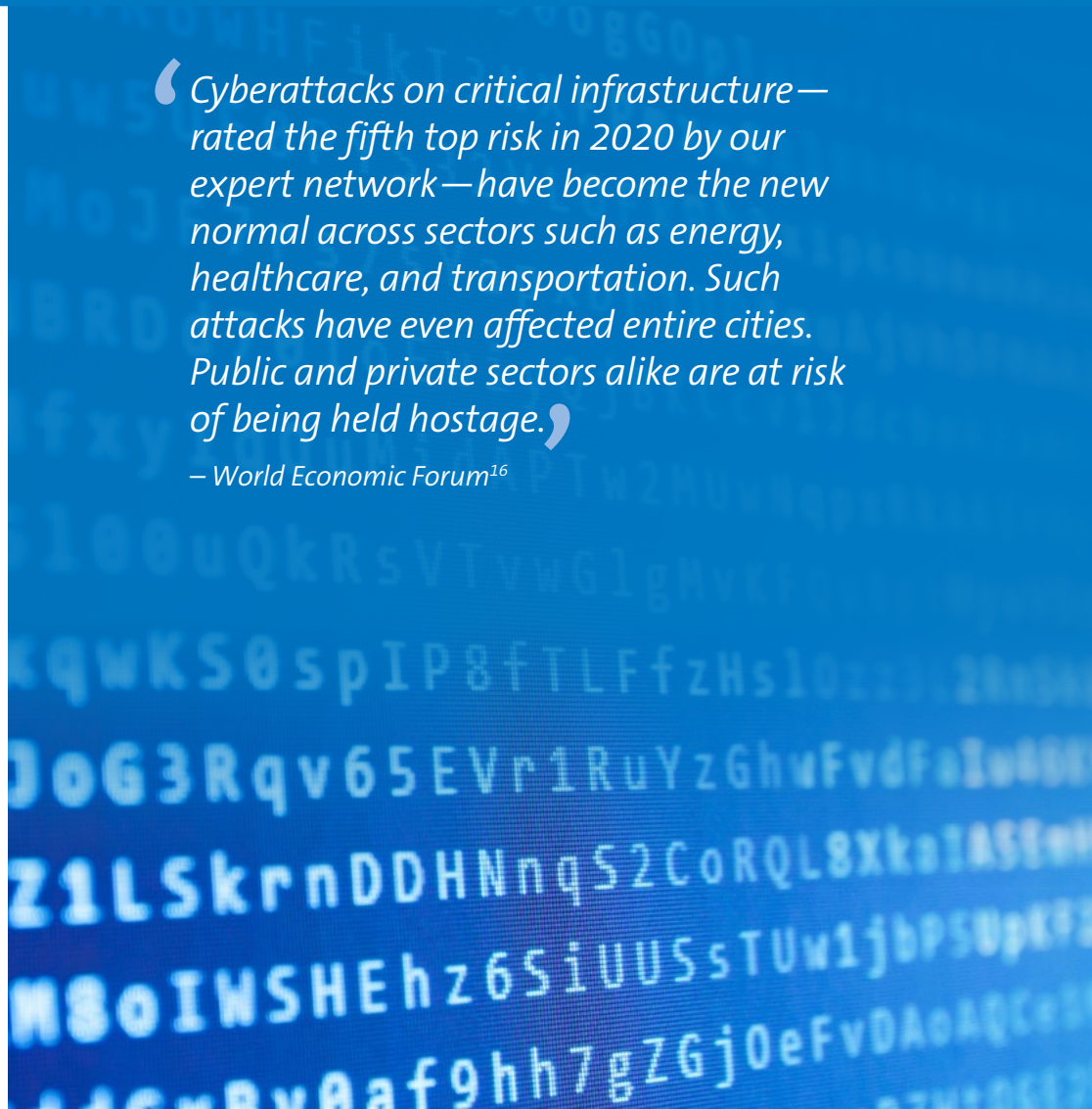
- The UK has finalised its operational resilience rules, which will require UK banks, financial services firms and market infrastructure to prepare for incidents and remain within pre-identified and limited tolerances for failure.
- In the US, in March 2022 a new law was passed requiring critical infrastructure to report significant cyber incidents within 72 hours and ransomware payments within 24 hours.
- The Office of the Comptroller of the Currency in the US (the ***US OCC***) has also recently published an order that provides a blueprint for the way organisations should be approaching cyber risk.
- The current war in Ukraine poses an increased cybersecurity threat to critical infrastructure, particularly as the 'spill over' risk of cybercrime is heightened.

Global enforcement action

- In the EU, fines for breach of the General Data Protection Regulation (GDPR) have ramped up recently, with Vodafone Italia being fined €12.3m for failing to properly secure customer data, and British Airways being fined €22m for a breach that compromised 400,000 customers' personal information (including names, addresses and payment information).
- The US OCC has issued a number of very large penalties for deficiencies in the cybersecurity and information-handling frameworks and protocols of financial services firms, including:
  - a US$400 million penalty against Citibank;
  - a US$85 million penalty against USAA, Federal Savings Bank;

"Cyberattacks on critical infrastructure—rated the fifth top risk in 2020 by our expert network—have become the new normal across sectors such as energy, healthcare, and transportation. Such attacks have even affected entire cities. Public and private sectors alike are at risk of being held hostage."

– World Economic Forum[16]



The US Securities and Exchange Commission proposes to mandate disclosure of cybersecurity incidents and risk management

Linklaters

The US Securities and Exchange Commission (the ***SEC***) has proposed regulations that would impose, for the first time as mandatory items, cybersecurity risk management, strategy, governance and incident disclosure rules on US public companies (including foreign private issuers), with the goal of enhancing and standardising disclosures regarding these items.

Specifically, the proposal would require disclosures about:

- material cybersecurity incidents, and updates on these incidents in annual and quarterly reports; and
- risk management, strategy and governance in annual reports and other periodic reports, including:
  - the company's policies and procedures to identify and manage cybersecurity risks;
  - management's role in implementing cybersecurity policies and procedures; and
  - the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk.

The SEC further notes that the discussion about cyber risk would include a discussion about 'the process by which the board is informed about cybersecurity risks and the frequency of its discussions on this topic'.

While the SEC does not propose requiring cyber expertise on the board, it is clear that the SEC is interested in such governance questions.

Materiality is defined in the proposed rule in a very different way than materiality to the company's performance. For example, the SEC suggests that an incident in which a hacker has demanded payment to restore company data is material, without any reference to the impact on the organisation.

Why is this important?

For directors, the requirement for incident notification means that the board must be notified earlier of cybersecurity incidents and be aware of incidents that may be disclosed to investors. Likewise, the requirement regarding risk disclosures means that the board will have to be well aware of the risk assessment process and the actions taken to remedy those risks.

Cybersecurity is an ESG issue

"As social identities become more defined by online identities, users will be increasingly at risk of exposure to targeted political manipulation, invasion of privacy, cybercrime, financial loss and psychological or physical harm"

– World Economic Forum Global Risks Report 2021[17]

Cyber resilience has now joined environmental, diversity and social justice issues on the ESG agenda. From unethical or misrepresented uses of data (eg the Cambridge Analytica affair), to major data breaches in the health and credit reporting sectors, to crippling cyberattacks on major supply chains (eg Solar Winds) – consumers are increasingly aware of the potential social and financial implications of deficient data and information security practices, and businesses are realising just how easy it can be to lose consumer trust.

This has spurred a demand for greater transparency, governance and reporting on cyber risk metrics, and we expect that reporting on cyber risk metrics (including on resilience to future adverse cyber events) will increasingly become a regulatory requirement.

6. Responding to ransomware attacks

2021 was a banner year for ransomware and cyber extortion – almost 33% of all companies experienced at least one cyber ransom incident, and ransomware attacks cost businesses more than $20 billion. Ransomware is now the fastest-growing and one of the most damaging types of cybercrime. Despite this, many businesses are still severely unprepared.

Given the potential damage (due to disrupted systems and leaked confidential data) these attacks can cause, and the ethical and legal complexities surrounding the payment of cyber ransoms, a company's response to any ransomware or cyber extortion attack is likely to attract intense scrutiny from regulators and other stakeholders.

How should directors prepare for a ransomware attack?

Directors should ensure that the company:

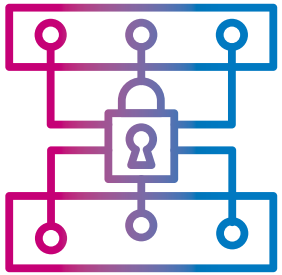
- has an easy-to-use ransomware and cyber extortion response and recovery plan, which covers (among other things) the extent of board involvement in decision making and how frequently the board will receive updates;
- understands the legality of paying a ransom in various scenarios, how best to approach the evolving sanctions landscape, and the cyber extortion notification requirements in the jurisdictions in which it operates;
- participates in regular ransomware and cyber extortion simulations; and
- knows which breach response experts (forensic, legal, communications and other experts) it will need to engage with and when.

What should directors do in the event of a ransomware or cyber extortion attack?

Directors should:

- ensure that all directors and senior executives are kept sufficiently informed about the detail of the attack and the response effort;
- consider advice from counsel and other third-party experts as to the risks of engaging with and/or paying a particular threat actor on an ongoing basis during the incident response – and make an independent assessment of such information or advice;
- satisfy themselves that any payment to a threat actor is lawful (or that they can rely on relevant defences), that the relevant compliance procedures have been adhered to and that records have been kept of these procedures; and
- ensure that all decisions made are based on a robust consideration of any risks identified, and are in line with the company's risk appetite and interests as a company. Directors will need to weigh risks such as the impact of customer data leaks and/or business interruption, exposure of the company to criminal offences and penalties, and damage to the company's reputation.

For more information about responding to ransomware attacks and data breaches, please get in touch with our team.



"Regulated companies should have an incident response plan that explicitly addresses ransomware attacks. The plan should be tested, and the testing should include senior leadership – decision makers such as the CEO should not be testing the incident response plan for the first time during a ransomware incident"

– New York Department of Financial Services[18]

7. Key contacts

HEAD OF CYBER

Valeska Bloch
Partner, Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

James Campbell
Partner
T +61 2 9230 4751
James.Campbell@allens.com.au

Chris Kerrigan
Partner
T +61 2 9230 4208
Christopher.Kerrigan@allens.com.au

Alex Mason
Partner
T +61 2 9230 4456
Alexandra.Mason@allens.com.au

Gavin Smith
Partner
T +61 2 9230 4891
Gavin.Smith@allens.com.au

Michael Park
Partner
T +61 3 9613 8331
Michael.Park@allens.com.au

Phil O'Sullivan
Partner
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au

David Rountree
Partner Elect
T +61 7 3334 3368
David.Rountree@allens.com.au

LINKLATERS

Erez Liebermann
Partner, Co-Chair of U.S. Data Solutions, Cybersecurity and Privacy Practice
T +1 212 903 9111
Erez.Liebermann@linklaters.com

Endnotes

1 Financial regulation in a digital world | ASIC - Australian Securities and Investments Commission
2 What the top five cybersecurity trends mean for your business in 2022 | Allens
3 What the top five cybersecurity trends mean for your business in 2022 | Allens
4 Executive Board Member Geoff Summerhayes - speech to Financial Services Assurance Forum | APRA
5 See ss 180, 181 and 182 of the *Corporations Act 2001* (Cth); s37CA of BEAR (the *Banking Act* 1959 (Cth)); ASIC REPORT 429: Cyber resilience: Health check (March 2015), which confirmed that directors duties under the Corporations Act extend to the conduct and operational risks of cyber resilience, privacy and data management; and the Australian Government's Cyber Security Strategy 2020, which moots the introduction of specific duties for company directors relating to cybersecurity.
6 See ss292 and 299, Corporations Act (reporting obligations); ASX Listing Rule 3.1 and s674A Corporations Act continuous disclosure obligations); and Recommendation 7.2 of the ASX Corporate Governance Principles and Recommendations.
7 See s18, Australian Consumer Law; s1041H, Corporations Act, ss12DA and 12DB, ASIC Act; s128, *Insurance Act 1973* (Cth); and s137.1, Criminal Code.
8 See s92(1)(b) and (d), the *Regulatory Powers (Standard Provisions) Act 2014* (Cth); and s84, the *Competition and Consumer Act 2010* (Cth) (consumer data right).
9 For example, s1309(2) of the Corporations Act creates a criminal offence with up to two years' imprisonment where a director or officer authorises or permits information that is false or misleading to be provided to the ASX without having taken reasonable steps to ensure that the information was not false or misleading.
10 Log4j: What Boards and Directors Need to Know | ACSC.
11 Australian Government, Strengthening Australia's cyber security regulations and incentives (2021).
12 Improving cyber resilience: the role boards have to play | APRA
13 'ASX 100 Cyber Health Check Report: Capturing the Opportunities While Managing the Threats, April 2017.
14 ParlInfo - BILLS : Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 : Second Reading (aph.gov.au)
15 Improving cyber resilience: the role boards have to play | APRA
16 World Wide Web – Consequences of Digital Fragmentation | World Economic Forum
17 The Global Risks Report 2021 | World Economic Forum
18 Industry Letter - June 30, 2021: Ransomware Guidance | Department of Financial Services (ny.gov)

19358D